

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-093546

(43)Date of publication of application : 10.04.1998

(51)Int.Cl.

H04L 9/10

G07D 7/00

G07F 7/08

H04L 9/08

(21)Application number : 08-247756

(71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 19.09.1996

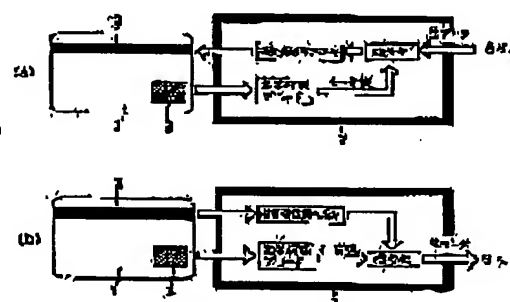
(72)Inventor : SAKAI MORIHITO
HORIGUCHI RYUJI

(54) CIPHERING SYSTEM USING INFORMATION RECORDING MEDIUM AND RECORDING MEDIUM FOR CIPHERED INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the inexpensive ciphering system with forgery preventing performance and an information recording medium such as a card by using information recorded on an optical information recording section so as to conduct ciphering and decoding of information to be recorded on other information recording section.

SOLUTION: Key information is read from an optical information recording section 3 of an information recording medium 1 provided with the optical information recording section 3 with the key information recorded thereon and other information recording section 2 and the key information is used to cipher input information according to the ciphering system and the ciphered information is recorded to the other information recording section 2, the ciphered information recorded to the other information recording section 2 is read and the information read from the other information recording section 2 is decoded according to the decoding formula by using the key information read from the optical information recording section 3.



LEGAL STATUS

[Date of request for examination]

31.07.2003

[Date of sending the examiner's decision of rejection]

22.02.2006

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-93546

(43) 公開日 平成10年(1998) 4月10日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 L 9/10

H 0 4 L 9/00

6 2 1 A

G 0 7 D 7/00

G 0 7 D 7/00

G 0 7 F 7/08

G 0 7 F 7/08

A

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 A

審査請求 未請求 請求項の数 8 O L (全 5 頁)

(21) 出願番号

特願平8-247756

(22) 出願日

平成 8 年 (1996) 9 月 19 日

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目 1 番 1 号

(72) 発明者 酒井守人

東京都新宿区市谷加賀町一丁目 1 番 1 号大

日本印刷株式会社内

(72) 発明者 堀口竜二

東京都新宿区市谷加賀町一丁目 1 番 1 号大

日本印刷株式会社内

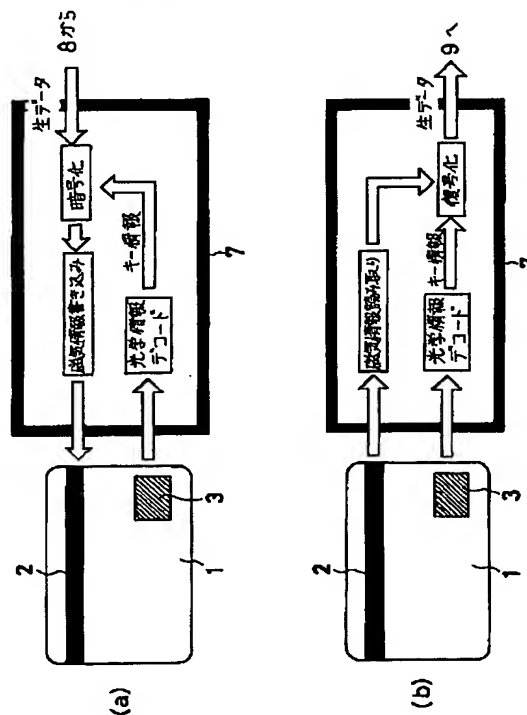
(74) 代理人 弁理士 荏澤 弘 (外 7 名)

(54) 【発明の名称】 情報記録媒体を用いた暗号化システム及び暗号化情報用記録媒体

(57) 【要約】

【課題】 光学情報記録部に記録された情報を用いて、他の情報記録部に記録する情報の暗号化と復号化を行うようにして、安価で高い偽造防止性の暗号化システムとカード等の情報用記録媒体。

【解決手段】 キー情報が記録された光学情報記録部 3 と他の情報記録部 2 とを備えた情報記録媒体 1 の光学情報記録部 3 からキー情報を読み取り、そのキー情報を用いて暗号式に従って入力情報を暗号化し、その暗号化情報を他の情報記録部 2 に記録すると共に、他の情報記録部 2 に記録されている暗号化情報を読み取り、光学情報記録部 3 から読み取られたキー情報を用いて復号式に従って、他の情報記録部 2 から読み取られた情報を復号化する。



【特許請求の範囲】

【請求項1】 キー情報が記録された光学情報記録部と他の情報記録部とを備えた情報記録媒体の前記光学情報記録部からキー情報を読み取り、そのキー情報を用いて暗号式に従って入力情報を暗号化し、その暗号化情報を前記の他の情報記録部に記録することを特徴とする情報記録媒体を用いた暗号化システム。

【請求項2】 キー情報が記録された光学情報記録部と他の情報記録部とを備えた情報記録媒体の前記光学情報記録部からキー情報を読み取り、また、前記の他の情報記録部に記録されている暗号化情報を読み取り、前記光学情報記録部から読み取られたキー情報を用いて復号式に従って、前記の他の情報記録部から読み取られた情報を復号化することを特徴とする情報記録媒体を用いた暗号化システム。

【請求項3】 キー情報が記録された光学情報記録部と他の情報記録部とを備えた情報記録媒体の前記光学情報記録部からキー情報を読み取り、そのキー情報を用いて暗号式に従って入力情報を暗号化し、その暗号化情報を前記の他の情報記録部に記録すると共に、前記の他の情報記録部に記録されている暗号化情報を読み取り、前記光学情報記録部から読み取られたキー情報を用いて復号式に従って、前記の他の情報記録部から読み取られた情報を復号化することを特徴とする情報記録媒体を用いた暗号化システム。

【請求項4】 キー情報が記録された光学情報記録部とそれと異なる他の情報記録部とを備えていることを特徴とする暗号化情報用記録媒体。

【請求項5】 前記の他の情報記録部には、前記光学情報記録部に記録されたキー情報を用いて暗号式に従って暗号化された情報が記録されていることを特徴とする請求項4記載の暗号化情報用記録媒体。

【請求項6】 前記光学情報記録部は、ホログラム又は回折格子から構成されていることを特徴とする請求項4又は5記載の暗号化情報用記録媒体。

【請求項7】 前記の他の情報記録部は、磁気記録媒体からなることを特徴とする請求項4から6の何れか1項記載の暗号化情報用記録媒体。

【請求項8】 カード形式であることを特徴とする請求項4から7の何れか1項記載の暗号化情報用記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報記録媒体を用いた暗号化システム及び暗号化情報用記録媒体に関し、特に、光学情報記録部と任意の方式の他の情報記録部とを備えた情報記録媒体を用いて暗号化と復号化を行う偽造防止システムとそのための暗号化情報用記録媒体に関するものである。

【0002】

【従来の技術】カード等に各種情報を記録する手段とし

て、磁気テープが一般的に用いられている。磁気テープは、専用のリーダーライターを使用することで、任意の情報の書き込み、読み取りを行うことができる。また、他の情報記録媒体であるICカード、光カード等と比較して安価なメリットを有している。

【0003】

【発明が解決しようとする課題】従来、磁気テープは、専用のリーダーライターなしには、情報の書き込み、読み取りができないことで、セキュリティ性を持たせている。しかし、偽造しようとする者がそのリーダーライターを入手した場合、簡単に情報の読み取り又は書き換えが可能となる。

【0004】実際、リーダーライターの入手はさほど難しくなく、磁気テープに記録されている情報が書き換えられる危険性は大きい。また、磁気の配向を変えてセキュリティ性を向上させる方法もあるが、高価になるという欠点がある。

【0005】本発明は従来技術のこのような問題点に鑑みてなされたものであり、その目的は、偽造防止性の高い光学情報記録部に記録された機械読み取り可能な情報を用いて、他の情報記録部に記録する情報の暗号化と復号化を行うようにして、安価で高い偽造防止性の暗号化システムと情報用記録媒体を提供することである。

【0006】

【課題を解決するための手段】上記目的を達成する本発明の情報記録媒体を用いた暗号化システムは、キー情報が記録された光学情報記録部と他の情報記録部とを備えた情報記録媒体の前記光学情報記録部からキー情報を読み取り、そのキー情報を用いて暗号式に従って入力情報を暗号化し、その暗号化情報を前記の他の情報記録部に記録することを特徴とするものである。

【0007】本発明のもう1つの情報記録媒体を用いた暗号化システムは、キー情報が記録された光学情報記録部と他の情報記録部とを備えた情報記録媒体の前記光学情報記録部からキー情報を読み取り、また、前記の他の情報記録部に記録されている暗号化情報を読み取り、前記光学情報記録部から読み取られたキー情報を用いて復号式に従って、前記の他の情報記録部から読み取られた情報を復号化することを特徴とするものである。

【0008】本発明のさらにもう1つの情報記録媒体を用いた暗号化システムは、キー情報が記録された光学情報記録部と他の情報記録部とを備えた情報記録媒体の前記光学情報記録部からキー情報を読み取り、そのキー情報を用いて暗号式に従って入力情報を暗号化し、その暗号化情報を前記の他の情報記録部に記録すると共に、前記の他の情報記録部に記録されている暗号化情報を読み取り、前記光学情報記録部から読み取られたキー情報を用いて復号式に従って、前記の他の情報記録部から読み取られた情報を復号化することを特徴とするものである。

【0009】また、本発明の暗号化情報用記録媒体は、キー情報が記録された光学情報記録部とそれと異なる他の情報記録部とを備えていることを特徴とするものである。

【0010】この場合、他の情報記録部には、光学情報記録部に記録されたキー情報を用いて暗号式に従って暗号化された情報が記録されているのが使用形態である。

【0011】光学情報記録部は、ホログラム又は回折格子から構成されていることが望ましい。また、他の情報記録部は、磁気記録媒体からなることが1つの形態である。なお、本発明の暗号化情報用記録媒体は、カード形式とすることができる。

【0012】本発明においては、光学情報記録部に用いられるホログラム等の偽造が困難なため、カード形式等の情報用記録媒体の偽造を防止することができると共に、他の情報記録部に記録されている情報が光学情報記録部に記録されたキー情報を用いて暗号化されているので、改竄することが困難である。また、暗号化、復号化のための装置を、光学情報記録部用の光学情報読み取り装置と一体化することで、暗号化、復号化のためのアルゴリズムを解読することが困難となる。

【0013】

【発明の実施の形態】以下に、本発明の情報記録媒体を用いた暗号化システム及び暗号化情報用記録媒体の実施例について説明する。この実施例は、カード上の磁気テープに記録される情報を、ホログラムあるいは回折格子からなる光学情報記録部に記録された情報をキーとして、暗号化、復号化する実施例である。図1にシステム構成を、図2に暗号化(a)、復号化(b)する際の信号の流れを示す。

【0014】カード1は、磁気テープ2と光学情報記録部3を有する。図1の場合、磁気テープ2の領域と光学情報記録部3の領域とをカードの1面上の別々の領域としているが、相互に重なるようにしても、別々の面の上に配置するようにしてもよい。また、光学情報記録部3としては、ホログラムに光電的に読み取り可能なバーコード形態等の情報が記録されているもの(例えば、特開昭62-283384号)、回折格子で構成された光電的に読み取り可能なバーコード形態等の情報が記録されているもの(例えば、特願平3-327683号)等があり、何れの形態でもよい。そして、光学情報記録部3には、情報暗号化のためのキー情報が固定記録されている。

【0015】このようなカード1の磁気テープ2への記録情報の暗号化、及び、磁気テープ2に記録された暗号化情報を復号化する情報暗号化・復号化装置10は、磁気テープ2から記録情報を読み取ったり記録する磁気ヘ

ッド4、光学情報記録部3へ読み取り照明光を照射する読み取り光源5、光源5からの照明光で照射され、光学情報記録部3で回折、散乱等がされた光を受光してそこに記録されているキー情報を読み取る光学情報読み取りセンサー6、暗号化・復号化処理回路7、情報入力装置8、表示装置9からなる。

【0016】この情報暗号化・復号化装置10を用いて、カード1の磁気テープ2へ暗号化情報を記録するには、図2(a)に示すように、光源5から照明光をカード1の光学情報記録部3へ当て、そこからの回折光あるいは散乱光を光学情報読み取りセンサー6で読み取り、その読み取り信号を暗号化・復号化処理回路7へ入力してデコード処理を施して、キー情報を得る。一方、情報入力装置8から生データ(記録すべき情報)を入力し、上記の光学情報記録部3から読み取ったキー情報を用いて、所定の暗号式に従って情報入力装置8から入力した生データを暗号化処理する。暗号化情報は、磁気ヘッド4を経て磁気テープ2へ記録する。

【0017】また、磁気テープ2に記録されているこのような暗号化情報を読み取って復号化して元の生データを得るには、図2(b)に示すように、暗号化の時と同様に、光源5から照明光をカード1の光学情報記録部3へ当て、そこからの回折光あるいは散乱光を光学情報読み取りセンサー6で読み取り、その読み取り信号を暗号化・復号化処理回路7へ入力してデコード処理を施して、キー情報を得る。同時に、磁気ヘッド4により磁気テープ2に記録されている暗号化情報を読み取り、上記の光学情報記録部3から読み取ったキー情報を用いて、所定の復号式に従って復号化処理を施すことにより、元の生データが得られる。得られた情報を例えば表示装置9に表示することにより、暗号化されて記録された元の情報が復号化されて可視化される。

【0018】上記の暗号式、復号式は対になっていて任意に設定でき、関係者しか分からないものであるから、カードにキー情報が記録されていても、他の者は磁気テープ2に記録されている情報を正しく復号化できないと共に、磁気テープ2に記録する暗号化情報を偽造することもできず、したがって、安価な構成で高い偽造防止性が得られる。

【0019】次に、簡単な実例として、1つの暗号化とその復号化の例を示す。平文(元情報)及び鍵(キー情報)は、共に、図3に示すようなキャラクターコード表で与えられるASCIIコードの30h(0)から7Ah(z)を使用するものとする。暗号化ルーチンの1例として、下式を用いた場合について説明する。

【0020】

暗号式: $\sim \{ (\text{平文}) \text{ XOR } (\text{鍵}) \}$. . . ①

復号式: $\sim \{ (\text{暗号文}) \} \text{ XOR } (\text{鍵})$. . . ②

ここで、 $\sim \{ \}$ はカッコ内の情報の否定とし、1例と

して、平文を“DNP”(44h, 4Eh, 50h)と

し、鍵を“ABC”(41h, 42h, 43h)とすると、上記の暗号式①を用いて演算すると、後記のように、下記の暗号文が得られる。

【0021】暗号文: FAh, F3h, Ech

<暗号化>

平 文	4	4	4	E	5	0
平 文	0100	0100	0100	1110	0101	0000
鍵	0100	0001	0100	0010	0100	0011
(平文) XOR (鍵)	0000	0101	0000	1100	0001	0011
～{(平文) XOR (鍵)}	1111	1010	1111	0011	1110	1100
暗号文	F	A	F	3	E	C

<暗号化>

暗号文	F	A	F	3	E	C
暗号文	1111	1010	1111	0011	1110	1100
～{(暗号文)}	0000	0101	0000	1100	0001	0011
鍵	0100	0001	0100	0010	0100	0011
～{(暗号文)} XOR (鍵)	0100	0100	0100	1110	0101	0000
平 文	4	4	4	E	5	0

平文及び鍵は前記のように、先頭が必ず「3」～「7」であるのに対して、暗号文は必ず「8」～「F」になるので、両者は明確に区別可能であると共に、暗号文はASCIIコードで用いないキャラクターを用いることになるので、磁気テープ2に記録されている情報が暗号化情報であることが直ぐに判別可能である。

【0023】なお、本発明において、磁気テープの代わりに、ICメモリ、磁気光学記録媒体等少なくとも書き込み可能な情報記録媒体なら公知の任意の方式の情報記録媒体を用いることができる。また、本発明による情報記録媒体は、カード形式に限らず通帳等他の形式のものであってもよい。また、キー情報を用いて暗号式、復号式に従って暗号化、復号化する手法には、DES等多くのものがあり、当然ながら何れを用いてもよい。

【0024】

【発明の効果】以上の説明から明らかなように、本発明の情報記録媒体を用いた暗号化システム及び暗号化情報記録媒体によると、光学情報記録部に用いられるホログラム等の偽造が困難なため、カード形式等の情報記録媒体の偽造を防止することができると共に、他の情報記録部に記録されている情報が光学情報記録部に記録されたキー情報を用いて暗号化されているので、改竄することが困難である。また、暗号化、復号化のための装置

また、上記の暗号文を復号式②を用いて演算すると、下記のように、平文“DNP”が得られる。

【0022】

を、光学情報記録部用の光学情報読み取り装置と一体化することで、暗号化、復号化のためのアルゴリズムを解読することが困難となる。したがって、安価で高い偽造防止性の暗号化システムと情報用記録媒体が得られる。

【図面の簡単な説明】

【図1】本発明の情報記録媒体を用いた暗号化システムの1実施例のシステム構成図である。

【図2】図1のシステムにおける暗号化と復号化の際の信号の流れを示す図である。

【図3】ASCIIコードのキャラクターコード表を示す図である。

【符号の説明】

- 1…カード
- 2…磁気テープ
- 3…光学情報記録部
- 4…磁気ヘッド
- 5…読み取り光源
- 6…光学情報読み取りセンサー
- 7…暗号化・復号化処理回路
- 8…情報入力装置
- 9…表示装置
- 10…情報暗号化・復号化装置

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.